International Journal of Science and Research Archive

eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(Research Article)

Focus group meeting results on cybersecurity in midstream operations: Integrating emerging technologies with legacy infrastructure

Ismail D. Gunes [1, 2, *]

[1] *Department of Homeland Security & Criminal Justice.*
[2] *Sul Ross State University, Alpine, TX.*

International Journal of Science and Research Archive, 2025, 16(03), 1218-1225

Publication history: Received on 19 August 2025; revised on 25 September 2025; accepted on 27 September 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.3.2703

Abstract

The midstream energy sector faces escalating cybersecurity challenges due to the increasing sophistication of cyber threats and the complexity involved in integrating modern security technologies into aging infrastructures. This paper explores a multi-faceted approach to cybersecurity in midstream operations, drawing insights from focus group discussions and scholarly literature. It discusses key technologies such as Zero Trust architecture, network segmentation, and the role of cloud services while also highlighting the critical challenges associated with legacy systems. The study provides a layered analysis of threat detection strategies, vulnerabilities in operational technology (OT), and the applicability of artificial intelligence (AI) and automation in industrial control environments. By synthesizing current practices and challenges, this paper presents a comprehensive view of how midstream operators can cultivate a resilient cybersecurity posture to safeguard critical infrastructure.

Keywords: Cybersecurity; Midstream Operations; Operational Technology (OT); Threat Detection; Data Protection.

1. Introduction: Cybersecurity in the Oil and Gas Industry

Cybersecurity has increasingly become an indispensable pillar in the oil and gas industry, given the sector's foundational role in global economic stability, its growing reliance on digital technologies, and the rising sophistication of cyber threats. This synthesis underscores the urgency of implementing robust cybersecurity practices, as evidenced by current literature.

The oil and gas sector serves as a cornerstone of the global economy, characterized by high levels of interconnectivity and dependence on advanced technological systems [1]. The integration of digital technologies across operational technology (OT) and information technology (IT) systems has yielded substantial efficiencies. However, this digital transformation has simultaneously exposed critical infrastructure to a broader and more aggressive threat landscape. As emphasized by Stergiopoulos et al. [2], these developments have rendered the industry a lucrative target for cyber adversaries seeking to exploit vulnerabilities in interconnected systems. The ramifications of such attacks can be severe, ranging from operational halts and equipment damage to environmental disasters and significant financial losses. This reality underscores the vital importance of proactive cybersecurity measures to ensure operational continuity and protect national and economic interests [3].

In this context, structured cybersecurity frameworks are essential. The NIST Cybersecurity Framework, for instance, offers a systematic methodology for identifying, protecting against, detecting, responding to, and recovering from cyber threats [4]. Such frameworks function as blueprints for organizations to institute resilience in their digital infrastructure and respond effectively to an increasingly dynamic threat environment.

[*] Corresponding author: Ismail D. Gunes

Moreover, the integration of emerging technologies, including the Internet of Things (IoT) and 5G networks, into oil and gas operations presents both opportunities and risks. These technologies promise enhanced efficiency, real-time monitoring, and improved decision-making capabilities. However, as highlighted by Ikemefuma et al. [5], they also introduce a plethora of new cybersecurity vulnerabilities, including insecure IoT endpoints and increased attack surfaces. Addressing these challenges necessitates a forward-looking and adaptive cybersecurity posture that evolves alongside technological advancements. Without such measures, the operational and strategic benefits of digital transformation cannot be fully realized [6].

Another critical aspect of cybersecurity in the sector pertains to the geographic and operational complexity of oil and gas infrastructure. Many facilities, including offshore platforms and remote field installations, operate in isolated and often inhospitable environments, complicating the implementation of traditional IT security protocols and magnifying the risk of undetected or delayed cyber intrusions. Remote systems frequently rely on automated control networks and are interconnected with extensive global supply chains, which are major factors that necessitate customized and robust cybersecurity solutions [3]. Zhu and Liyanage [7] further underscore the need for industry-specific strategies that consider the operational constraints and unique risk profiles of such locations.

In conclusion, the critical importance of cybersecurity in the oil and gas sector derives not only from the industry's economic significance but also from the evolving threat landscape and the accelerating pace of digital transformation. To safeguard operational integrity and ensure long-term sustainability, the industry must invest in comprehensive cybersecurity strategies responsive to both current and emerging risks. This includes implementing proven frameworks, conducting continuous risk assessments, and aligning security practices with technological innovations. By doing so, the oil and gas sector can reinforce its resilience, mitigate potential disruptions, and maintain its pivotal role in the global energy ecosystem.

2. Research Method: Focus Group Discussion

The "Midstream Critical Manufacturing Industry Cybersecurity Hub" is a strategic research initiative funded by the U.S. Department of Energy. This multidisciplinary project represents a collaborative effort between Sul Ross State University (SRSU) and Lamar University (LU), located strategically in key oil-producing and refining regions of Texas. The project aims to enhance cybersecurity resilience across midstream critical manufacturing sectors integral to the nation's oil and gas infrastructure.

2.1. Sul Ross State University (SRSU) and the Permian Basin Region

SRSU, with its main campus in Alpine, Texas, is situated in the western region of the state, adjacent to the Permian Basin, which is one of the largest and most productive hydrocarbon-producing basins in the United States. The Permian Basin has historically been a cornerstone of U.S. oil production and continues to play a vital role in its contemporary energy output, accounting for over 50% of all active drilling rigs in the nation. Projections suggest it may contribute up to 50% of total U.S. oil production by 2030. This region contains extensive energy infrastructure, including pipelines, gas processing plants, and oil field operations, representing approximately 10% of Texas's statewide pipeline infrastructure and 21% of its midstream gas processing facilities. The strategic importance of SRSU's participation in a cybersecurity initiative focused on midstream systems is underscored by its location within the Permian Basin.

2.2. Lamar University (LU) and the Southeast Texas Petrochemical Corridor

LU, located in Beaumont, Texas, is situated within one of the most concentrated petrochemical and refining corridors in the United States. Southeast Texas serves as a hub for downstream and midstream operations, with significant infrastructure encompassing refineries, chemical plants, liquid natural gas (LNG) terminals, and offshore oil and gas facilities. Beaumont's historical link to the birth of the modern oil industry through the Spindletop oil boom of 1901 continues to shape the region's economic and industrial identity. LU's location within a 20-mile radius of over 75 refineries and petrochemical facilities positions it exceptionally well for industrial collaboration and research. Its proximity to the Port of Beaumont, the fourth largest U.S. port by tonnage and the nation's premier LNG export hub, further enhances its role in supporting the global energy market. The collaborative effort between SRSU and LU through the "Midstream Critical Manufacturing Industry Cybersecurity Hub" leverages their geographic, industrial, and academic positioning to address critical cybersecurity challenges within the midstream sector. By anchoring the initiative in regions with deep-rooted ties to oil and gas infrastructure, the project is well-positioned to yield impactful research outcomes, develop workforce training pipelines, and support the resilience of national energy systems.

2.3. Data Collection

The data collection strategy for this research project involved three structured focus group sessions designed to investigate current technologies, evaluate the effectiveness of existing cybersecurity measures, identify emerging solutions, and explore threat-mitigation strategies specific to midstream operations in the energy sector. The initial focus group session took place in person on February 21, 2025, in Houston, Texas, which is a major hub for the midstream industry. Eight professionals were selected through purposive sampling following an extensive search within the industry; participants were chosen based on their specialized expertise and substantial hands-on experience in operational technology (OT) and cybersecurity. Their professional roles included OT engineers, network architects, and IT security specialists, each responsible for their respective organization's cybersecurity posture.

To promote informed dialogue, participants received a set of discussion questions in advance of the initial meeting. This pre-distribution was intended to encourage reflective engagement and facilitate a productive discussion. The in-person meeting lasted approximately four hours and was moderated by a trained facilitator experienced in leading technical focus groups. The session followed a semi-structured format, allowing for open exchanges while adhering to a guiding framework. This foundational meeting built rapport among participants and familiarized them with the collaborative nature of the research, setting the stage for two subsequent virtual focus group sessions held on March 28, 2025, and May 30, 2025. Each online session lasted approximately two hours, using a secure video conferencing platform to ensure accessibility and confidentiality. Throughout all sessions, participants engaged in substantive discussions related to evolving cybersecurity threats, response strategies, technology implementation challenges, and organizational practices concerning midstream operations. All meetings were audio-visually recorded with consent from participants, and comprehensive notes were taken to support subsequent analysis. Participation was voluntary, and all individuals received compensation for their time and contributions per the terms of the research grant.

2.4. Focus Group Discussions on Cybersecurity

Focus group discussions (FGDs) represent a qualitative research methodology that is extensively utilized across diverse disciplines, including the evolving sector of cybersecurity. By fostering interactive dialogues among participants, FGDs offer a unique avenue to gain deep insights into individual and collective perspectives. In cybersecurity, where stakeholder experiences, perceptions, and concerns vary significantly, FGDs can unveil the nuanced realities often obscured in more structured or quantitative approaches.

A prominent advantage of FGDs lies in their capacity to generate rich, dialogic exchanges, facilitating an exploration of multifaceted perspectives. This interactive environment not only encourages open expression but also promotes collaborative knowledge construction through group dynamics. Gamhewage et al. [8] underscore that FGDs enable critical stakeholders, such as government officials, IT professionals, and healthcare providers, to engage in reflective, contextualized conversations that lead to the identification of unique challenges and opportunities within their operational landscapes. Such tailored discussions prove particularly valuable in cybersecurity, where threats and responses can differ drastically across sectors.

Moreover, Richard et al. [9] highlight the inclusive nature of FGDs, which effectively elicit input from individuals who may be less inclined to contribute in formal or hierarchical settings. This inclusiveness is especially pertinent in cybersecurity education, where students and non-experts might hesitate to voice concerns or misconceptions in traditional interviews. By contrast, FGDs provide a relaxed and egalitarian setting, which can uncover previously unexpressed attitudes and learning barriers. Further supporting this collaborative benefit, Scheelbeek et al. [10] note that FGDs can tap into shared experiences and communal narratives, often yielding insights transcending individual accounts. This collective sense-making is instrumental in identifying systemic cybersecurity challenges, such as organizational culture, user behavior, and policy gaps, that might remain hidden in isolated interviews. Through iterative discussion and mutual engagement, participants can clarify concepts, question assumptions, and refine ideas, ultimately producing a layered understanding of cybersecurity concerns.

Despite their strengths, FGDs are not without limitations. A primary drawback is the risk of dominance within the group setting, whereby more outspoken participants may unintentionally overshadow others, resulting in imbalanced data collection. Barbour [11] emphasizes that the quality of moderation is critical to mitigating such issues. A skilled facilitator must actively manage dynamics to ensure all voices are heard and that discussions remain focused and inclusive. Logistical challenges also complicate FGD utilization in cybersecurity research. Organizing a representative and diverse cohort, particularly those with varying technical expertise, can be challenging due to scheduling conflicts, geographic dispersion, and participant availability. Furthermore, considering the rapidly changing nature of the cybersecurity landscape, discussions must be timely to remain relevant; delays may result in data becoming outdated or misaligned with current threats and technologies.

Another concern involves the potential for cognitive overload or miscommunication during discussions of complex cybersecurity topics. Participants may possess varying levels of familiarity with technical terminology or cyber-related concepts, leading to confusion or superficial engagement. In such instances, the collaborative setting, which is usually a strength of FGDs, can become a liability. Additionally, the group format may deter candid disclosure of personal experiences on sensitive topics such as breaches, errors, or non-compliance. Sim and Waterfield [12] argue that a lack of space for individual reflection might hinder the depth and authenticity of insights shared, particularly in areas of privacy concern.

In summary, FGDs offer valuable methodological advantages for cybersecurity research by allowing researchers to capture rich, interactive, context-sensitive data. Their strengths lie in fostering collaboration, revealing diverse perspectives, and facilitating deeper understanding of stakeholder experiences. However, notable challenges, including group dynamics, logistical hurdles, and subject-matter complexity, can affect the validity and comprehensiveness of findings. Through the comprehensive examination of these issues, the qualitative data obtained from the focus group discussions provide a critical foundation for the thematic analysis presented in the subsequent section.

3. Analysis of the Focus Group Discussions

The discourse surrounding cybersecurity in midstream operations revolves around a multi-faceted approach, with a focus on technology integration, evaluation of existing systems, emerging tools, and the enduring challenges posed by legacy infrastructures. As the energy sector faces increasingly sophisticated and targeted cyber threats, the implementation of robust cybersecurity practices has transitioned from a best practice to a strategic imperative. This thematic analysis synthesizes findings from focus group discussions, incorporating various scholarly references to provide an overview of the cybersecurity landscape within midstream operations. The findings are articulated under six thematic topics.

3.1. Cybersecurity Technologies in Midstream Operations

In midstream operations, where the secure transportation and storage of energy resources such as oil and natural gas are critical, cybersecurity plays a vital role in maintaining operational integrity and national security. Several technologies have gained prominence due to their effectiveness in addressing sector-specific risks. Network Access Control (NAC) is fundamental, ensuring that only authorized users and devices can interact with the network represents the first line of defense in a layered security model, effectively reducing exposure to insider threats and unauthorized external access [13]. With the evolution of cyber threats, NAC systems must adapt to dynamic access environments across remote terminals and mobile platforms used in field operations.

Network Detection and Response (NDR) technologies are crucial for identifying malicious activities within networks. In midstream operations, where diverse communication protocols such as DNP3, Modbus, and OPC are prevalent, NDR solutions must be highly adaptable to effectively detect anomalies across heterogeneous systems. The increasing volume of telemetry and data flows necessitates advanced analytics and behavior-based detection mechanisms to differentiate between benign and malicious activity.

The adoption of the Zero Trust model signifies a paradigm shift in cybersecurity strategies, particularly as it transcends perimeter-based defenses. Through identity verification at every access point and continuous validation of users and devices, Zero Trust architectures are increasingly embedded into midstream systems through specialized software solutions [14]. This approach aligns well with the decentralized and remote-access nature of midstream operations. Although Multi-Factor Authentication (MFA) has become standard for securing user access, its integration into legacy operational systems may inadvertently introduce vulnerabilities. Incompatibilities between modern MFA solutions and older control systems can lead to misconfigurations that expose systems to attack vectors. This complexity necessitates cautious deployment, often requiring MFA to be incorporated within a broader Zero Trust framework to ensure security without impairing functionality.

Furthermore, whitelisting, which is an approach that permits only approved software or commands, presents challenges in OT environments where operational continuity is paramount. The dynamic nature of system updates combined with the need for real-time responses often conflicts with rigid whitelisting policies, creating friction between security and functionality. Addressing this requires context-aware whitelisting practices that adjust to operational nuances.

3.2. Assessing Cybersecurity Tools for Critical Infrastructure

Evaluating the effectiveness of cybersecurity tools within midstream infrastructure must account for the unique characteristics of critical assets such as pipelines, control systems, and field devices. This evaluation involves a layered defense-in-depth approach, utilizing multiple overlapping controls to manage various attack vectors. Regular security audits and compliance tracking are foundational to maintaining cybersecurity readiness, allowing organizations to identify configuration drift, unauthorized changes, and lapses in policy enforcement [15]. Given the critical nature of midstream infrastructure, these assessments must be thorough and recurring, driven by both regulatory compliance and internal risk assessments.

One key concern is the reliance on manual interventions in cybersecurity workflows. These interventions are susceptible to human error, resulting in inconsistent policy application across distributed systems [16]. Therefore, increasing automation in threat response and policy enforcement is essential to ensure uniformity and speed in addressing security incidents. While artificial intelligence (AI) is often touted as a solution for cybersecurity monitoring and incident detection, its application in OT settings remains contentious. Many experts argue that AI solutions, typically trained on IT datasets, lack the contextual understanding necessary for OT-specific behaviors, inevitably leading to false positives or missed threats. Thus, organizations must take a measured approach to AI adoption, integrating it where suitable but refraining from over-reliance on its current capabilities in OT environments.

3.3. Addressing ICS and OT Cybersecurity Threats

As Industrial Control Systems (ICS) and Operational Technology (OT) increasingly become targets for cyberattacks, a specialized layered defense strategy becomes essential. This strategy includes tailored intrusion detection, network segmentation, and protocol-specific protections. Intrusion Detection Systems (IDS) must be integrated within an Operational Technology Demilitarized Zone (OT DMZ) to serve as a buffer between enterprise IT and sensitive OT networks. These IDS systems should be configured to understand and analyze specific protocols like Modbus or Profibus, rather than relying solely on generic IT-centric detection models. Protocol awareness significantly enhances threat detection accuracy and minimizes false alerts.

A common vulnerability in many environments arises from inadequate network segmentation, where flat networks also permit lateral movement for adversaries. Properly designed gateways, firewalls, and segmentation policies can mitigate this risk by isolating critical zones and enforcing access control between them. Segmentation should not be static; rather, it should be a dynamic, policy-driven model that adapts to operational requirements and threat intelligence.

Historically, the air-gap model has been the standard for securing industrial environments by physically isolating systems from external networks. However, this approach has proved inadequate due to modern connectivity demands. Innovations such as air-lock models, which permit controlled data flows with strict filtering, are gaining prominence as more practical and yet secure alternatives [17]. These methods enable secure information exchange while maintaining isolation principles, thus balancing security and operational practicality.

3.4. Challenges of Integrating New Technologies with Legacy Systems

Legacy systems present significant challenges to cybersecurity enhancement efforts in midstream operations. Many were not designed with security as a priority and struggle to accommodate modern defenses. A substantial portion of operational infrastructure continues to rely on outdated operating systems and hardware platforms that no longer receive vendor support. This lack of patching capability creates persistent vulnerabilities and necessitates the deployment of compensating controls such as network isolation, strict access control, and real-time monitoring. However, these are often temporary measures, requiring long-term strategic upgrade plans.

Supervisory Control and Data Acquisition (SCADA) systems, which are vital to midstream operations, demand particular attention. Developing comprehensive disaster recovery plans is essential for ensuring business continuity, enabling organizations to quickly restore hardware, software, and critical configurations following cyber incidents. Such plans must undergo routine testing and updates in alignment with evolving system architectures and threat profiles. Furthermore, latency emerges as a crucial factor when considering the adoption of cloud services for control and monitoring. Many SCADA applications necessitate near real-time performance, which cloud-hosted systems may struggle to consistently provide. Therefore, organizations must evaluate latency-sensitive applications thoughtfully before migrating, especially when timing delays could jeopardize safety or operational integrity.

3.5. Role of Cloud Services in Cybersecurity Strategy

The integration of cloud services into midstream cybersecurity strategies introduces both opportunities and risks. Although cloud platforms offer scalability, flexibility, and centralized visibility, they concurrently raise concerns over latency, security, and reliability, particularly in environments where high uptime and minimal response latency are requisite. Latency is a primary concern in OT applications, where even milliseconds of delay can have critical operational consequences. Real-time processing demands can strain cloud infrastructure, particularly when connectivity is unstable or when engaging remote assets. Hybrid architectures are emerging to alleviate this challenge, combining local edge computing with centralized cloud resources.

To mitigate risks, companies must enforce end-to-end encryption throughout the data lifecycle. Encryption at rest, in transit, and during processing aids in preventing unauthorized access and data breaches, especially when utilizing third-party cloud services. Containerization technologies provide additional layers of protection. By isolating applications and their dependencies within containers, organizations can impose stricter security boundaries, minimize attack surfaces, and conduct rapid incident response through redeployment. Nonetheless, implementing containerization in OT systems requires careful planning to avoid operational disruptions and ensure compatibility with existing vendor systems. The complexity of cloud integration in control systems highlights the necessity for a tailored approach, one considerate of real-time demands, regulatory compliance, and operational resiliency.

3.6 Threat Detection and Monitoring within Distributed Assets

The geographic distribution of midstream assets, such as pipelines, terminals, and compressor stations, introduces considerable challenges in threat monitoring and detection. These environments necessitate a centralized yet context-sensitive cybersecurity strategy. Many organizations deploy Security Operations Centers (SOCs) that unify monitoring across IT and OT domains. These SOCs aggregate telemetry, threat intelligence, and log data to create holistic situational awareness. However, handling sensitive OT data within shared analytics platforms requires caution, especially within the confines of an OT DMZ where segmentation and security policies complicate data movement.

Debate exists between active and passive scanning within OT networks. Active scanning provides greater visibility but risks interference with sensitive control systems. Conversely, while passive scanning is safer, it may lack the depth required to detect stealthier threats or misconfigurations that active methods could uncover [18]. Consequently, many organizations are adopting a hybrid monitoring strategy, utilizing passive scanning for continuous baseline visibility while selectively employing active scanning during scheduled maintenance windows or in sandboxed environments to reduce operational risk.

Establishing baseline performance metrics is critical for enhancing threat detection accuracy. These baselines define normal system behavior, enabling cybersecurity teams to identify deviations that may signal a cyber intrusion or misconfiguration. Over time, these baselines must be updated to reflect system changes, infrastructure expansions, or the introduction of new technologies. The human element remains foundational to effective monitoring. Despite the sophistication of automation, skilled personnel are required to interpret anomalous events, fine-tune detection rules, and manage incident response protocols. As threat actors advance, relying solely on automated systems without human oversight can result in overlooked threats or an inundation of false positives. Regular training, tabletop exercises, and collaboration between IT and OT security teams are crucial for ensuring personnel’s adaptability to evolving threat landscapes.

4. Discussion

In summary, cybersecurity within midstream operations has transcended its status as a secondary concern to manifest as an operational imperative. As cyber threats continue to grow in complexity and potential impact, midstream operators must implement a comprehensive, layered, and adaptive approach to securing their infrastructure. This strategy should encompass embracing advanced technologies such as Zero Trust frameworks, specialized IDS systems, and cloud security architectures while remaining cognizant of legacy systems' practical limitations and associated risks.

It is equally essential to recognize that security is not static. Continuous evaluation, improvement, and alignment with evolving operational needs and threat intelligence are imperative. Effective cybersecurity in midstream operations does not stem solely from technology; it relies on strategic planning, skilled personnel, and organizational commitment across all levels. By methodically integrating emerging technologies, compensating for legacy constraints, and enhancing detection and response mechanisms, the energy sector can significantly bolster its cyber resilience. This ongoing evolution of security practices not only protects assets but also safeguards critical national infrastructure, environmental safety, and economic stability.

Compliance with ethical standards

Acknowledgments

The "Midstream Critical Manufacturing Industry Cybersecurity Hub" is a research project funded by the U.S. Department of Energy under grant number DE-CR0000037. Oguzhan Basibuyuk, Ph.D. (oguzhan.basibuyuk@sulross.edu) who is a Professor at Sul Ross State University is the Principal Investigator (PI) of this project. Helen H. Lou, Ph.D. (hhlou@lamar.edu) who is a Professor at Lamar University is the other Co-PI along with the author of this article. The author of this article, Ismail D. Gunes, Ph.D. (ismail.gunes@sulross.edu) is an Associate Professor at Sul Ross State University and also a Co-PI in this project.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Zand, M. (2024). The Economy of Oil and Gas Industry; A Comprehensive Study. 10.13140/RG.2.2.23715.36649.

[2] Stergiopoulos, G., Gritzalis, D. & Limnaios, E. (2020). Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3007960.

[3] Falco, G.J. (2018). Cybersecurity for Urban Critical Infrastructure. Ph.D. Dissertation. Available at: https://dspace.mit.edu/handle/1721.1/118226

[4] National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

[5] Ikemefuna, D., Yusuf, S. & Akinbi, I. (2025). Cybersecurity Challenges in The Oil And Gas Industry: Protecting Critical Infrastructure from Emerging Threats. International Research Journal of Modernization in Engineering Technology and Science. 10.56726/IRJMETS61881.

[6] Nazari, Z. & Musilek, P. (2023). Impact of Digital Transformation on the Energy Sector: A Review. Algorithms. 16. 211. 10.3390/a16040211.

[7] Zhu, P. & Liyanage, J.P. (2021). Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts: A Specific Review of Issues and Challenges in Safety Instrumented Systems. European Journal for Security Research. 6(2):125–49. doi: 10.1007/s41125-021-00076-2. Epub 2021 Dec 3. PMCID: PMC8639851.

[8] Gamhewage G., Mahmoud M.E., Tokar A., Attias M., Mylonas C., Canna S. & Utunen H. (2022). Digital Transformation of Face-To-Face Focus Group Methodology: Engaging a Globally Dispersed Audience to Manage Institutional Change at the World Health Organization. Journal of Medical Internet Research. 24(5): e28911. doi: 10.2196/28911. PMID: 35617007; PMCID: PMC9185345.

[9] Richard, B., Sivo, S., Orlowski, M., Ford, R., Murphy, J., Boote, D. & Witta, E. (2021). Qualitative Research via Focus Groups: Will Going Online Affect the Diversity of Your Findings?. Cornell Hospitality Quarterly. 62. 10.1177/1938965520967769.

[10] Scheelbeek, P. F. D., Hamza, Y. A., Schellenberg, J., & Hill, Z. (2020). Improving the use of focus group discussions in low-income settings. BMC Medical Research methodology. 20(1), 287. https://doi.org/10.1186/s12874-020-01168-8

[11] Barbour R. (2021). Doing Focus Groups. Sage Research Methods. https://doi.org/10.4135/9781526441836

[12] Sim, J. & Waterfield, J. (2019). Focus Group Methodology: Some Ethical Challenges. Quality & Quantity. 53, 3003–3022. https://doi.org/10.1007/s11135-019-00914-5

[13] CISCO Systems (2025). What Is Network Access Control? Available at: https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-access-control-nac.html

[14] Industrial Defender (2025). Zero Trust & Enforcing OT Security Inside the Perimeter. Available at: https://www.industrialdefender.com/blog/zero-trust-enforcing-ot-security-inside-the-perimeter#:~:text=Zero%20Trust%20requires%20full%20awareness,emphasizes%20tight%20segmentation%20between%20zones.

[15] Olutimehin, A.T. (2025). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and Its Applicability to Decentralized Finance (DeFi). SSRN. Available at: http://dx.doi.org/10.2139/ssrn.5133050

[16] Mohamed, N. (2025). Artificial Intelligence and Machine Learning in Cybersecurity: A Deep Dive into State-Of-The-Art Techniques and Future Paradigms. Knowledge and Information Systems 67, 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

[17] Rolan, G., Dalins, J. & Wilson, C. (2022). The Data Airlock: Infrastructure for Restricted Data Informatics. 10.48550/arXiv.2203.09006.

[18] Ecik, H. (2021). Comparison of Active Vulnerability Scanning vs. Passive Vulnerability Detection. 87-92. 10.1109/ISCTURKEY53027.2021.9654331.